桐柏县卫健委
网络与信息安全突发事件应急预案

一、总则

（一）目的

为提高我委处理网络与信息安全突发事件的能力，形成科学、有效、反应迅速的应急工作机制，更好地服务卫健系统工作，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减少网络与信息安全突发公共事件的危害，保护公众利益。

（二）适用范围

桐柏县卫健委发生和可能发生的网络与信息安全突发事件。

（三）工作原则

1.预防为主。立足安全防护，加强预警，重点保护基础信息网络和重要信息系统，从预防、监控、应急处理、应急保障和打击犯罪等环节，采取多种措施，共同构筑网络与信息安全保障体系。

2.快速反应。在网络与信息安全突发公共事件发生时，按照快速反应机制，及时获取充分而准确的信息，迅速处置，最大程度地减少危害和影响。

3.以人为本。把保障公共利益以及公民、法人和其他组织的合法权益的安全作为首要任务，及时采取措施，最大限度地避免公民财产遭受损失。

4.分级负责。按照“谁主管谁负责、谁使用谁负责”以及“条块结合”的原则，建立和完善安全责任制及联动工作机制。根据部门职能，各司其职，加强协调与配合，形成合力，共同履行应急处置工作的管理职责。

（四）编制依据

根据《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》及委有关规定，制定《网络与信息安全突发事件应急预案》（以下简称预案）。

二、组织机构及职责

（一）组织机构

成立桐柏县卫健委网络安全和信息化工作领导小组（负责网络与信息安全突发事件应急工作）

组　长：王诗庆主任

副组长：委有关班子成员

成　员：委各科室负责人及基层卫生健康和信息化股负责人。

应急处置工作组办公室设在基层卫生健康和信息化股。

（二）委网络与信息安全类突发事件应急处置工作职责

1.负责编制、修订委网络与信息安全突发事件应急预案。

2.通过国内外安全网络信息组织交流等手段获取安全预警信息，周期性或即时性地向局域网和用户网络管理部门发布；对异常流量来源进行监控，并妥善处理各种异常情况。

3.及时组织专业技术人员对委网络与信息安全突发事件的应急处置；负责网络与信息安全突发事件的调查和处置情况报告，并按照相关规定作好善后工作。

4.负责组建信息网络安全应急救援队伍并组织培训和演练。

三、预防及预警机制

网络与信息安全突发事件安全预防措施包括分析安全风险、准备应急处置措施，建立网络和信息系统的监测体系，控制有害信息的传播，预先制定信息安全重大事件的通报机制。

（一）网络与信息安全突发事件分类

关键设备或系统的故障；自然灾害（水、火、电等）造成的物理破坏；人为失误造成的安全事件；电脑病毒等恶意代码危害；人为的恶意攻击等。

（二）应急准备

基层卫生健康和信息化股和各单位信息管理员明确职责和管理范围，根据实际情况，安排应急值班，确保到岗到人，联络畅通，处理及时准确。

（三）具体措施

1.建立安全、可靠、稳定运行的机房环境，防火、防盗、防雷电、防水、防静电、防尘；建立备份电源系统；加强所有人员防火、防盗等基本技能培训。

2.实行实时监视和监测，采用认证方式避免非法接入和虚假路由信息。

3.重要系统采用可靠、稳定硬件，进行备份等措施，落实数据备份机制，遵守安全操作规范；安装有效的防病毒软件，及时更新升级扫描引擎；加强对卫健系统网内所有用户和信息管理员进行安全技术培训。

4.安装反入侵检测系统，监测攻击、病毒和蠕虫的发展，控制有害信息经过网络的传播，建立网关控制、内容过滤等控制手段。

四、有关应急预案

（一）机房漏水应急预案

1.发生机房漏水后，第一目击者应立即通知基层卫生健康和信息化股。

2.若空调系统出现渗漏水，应立即停止故障空调,将机房内的积水清除干净，并及时联系设备供应方进行处理，同时启动备用空调，必要情况下可以临时用电扇对服务器进行降温。

3.若为墙体或窗户渗漏水，应立即通知后勤处，及时清除积水，进行墙体或窗户维修，避免不必要的损失。

（二）设备发生被盗或人为损害事件应急预案

1.发生设备被盗或有人为损害设备情况时，使用者或管理者应立即报告网络安全和信息化工作领导小组，同时保护好现场。

2.网络安全和信息化工作领导小组接报后，通知保卫科及公安部门，一同核实审定现场情况，清点被盗物资或盘查人为损害情况，做好必要的影像记录和文字记录。

3.事件当事人应当积极配合公安部门进行调查，并将有关情况向网络安全和信息化工作领导小组汇报。

4.网络安全和信息化工作领导小组召开会议研讨事态严重时，应向委党委报告，请示进一步处理的决策。

（三）机房长时间停电应急预案

1.接到长时间停电通知后，应急领导小组根据停电时间、电池电能贮备、供电管理部门信息、网络和信息运行情况等及时通过官方网站发布或电话作调度，要求用户在停电前停止业务、保存数据。

2.及时搞清停电原因及具体停电时间，如供电部门告知停电时间过长，应及时备份相关数据,关闭相关设备，保证业务数据不丢失，保证网络设备正常运转。

（四）通信网络故障应急预案

1.发生通信线路中断、路由故障、流量异常、域名系统故障后，值班员应及时通知委办公室和相关科室。

2.及时查清通信网络故障位置，告知相关通信网络运营商，要求查清原因，同时，隔离故障区域，切断故障区与服务器的网络联接。

3.会同相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

4.相关责任人负责写出故障分析报告，上报网络安全和信息化工作领导小组备查。

（五）不良信息和网络病毒事件应急预案

1.当发现不良信息或网络病毒时，信息管理员应立即断开网线，终止不良信息或网络病毒传播，并告知网络安全和信息化工作领导小组。

2.接到报告后，应立即通告委局域网内所有计算机用户防病毒方法，隔离网络，督促信息管理员进行杀毒处理，直至网络处于安全状态。

3.对不良信息要进一步追查来源，对未经相关领导同意，擅自发布信息，造成不良影响且触犯法律者，移交执法部门追究法律责任。

4.情况严重时，应立即向委党委报告，请求支援，作好应对措施；处置人员记录事件处理步骤和结果，汇总上报。

（六）服务器软件系统故障应急预案

1.发生服务器软件系统故障后，立即启动备份服务器系统，由备份服务器接管业务应用。

2.相关责任人将故障服务器脱离网络，保存系统状态不变，取出系统镜像备份磁盘，保持原始数据。

3. 基层卫生健康和信息化股在确认安全的情况下，重新启动故障服务器系统；重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商和上级单位，请求技术支援，作好技术处理。

（七）黑客攻击事件应急预案

1.当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告网络安全和信息化工作领导小组。

2.接到报告后，基层卫生健康和信息化股立即关闭服务器或系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

3.及时清理系统、恢复数据、程序，尽力将系统和网络恢复正常；情况严重的，应上报委党委，并请求支援。

（八）核心设备硬件故障应急预案

1.发生核心设备硬件故障后，基层卫生健康和信息化股立即确定故障设备及故障原因，并进行先期处置。

2.若故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

3.故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商，认真填写设备故障报告单备查。

（九）业务数据损坏应急预案

1.发生业务数据损坏时，基层卫生健康和信息化股应及时检查、备份业务系统当前数据。

2.调用备份服务器备份数据。

3.业务数据损坏事件超过2小时后，基层卫生健康和信息化股应及时通知科室以手工方式开展业务。

4.待业务数据系统恢复后，检查历史数据和当前数据的差别，由相关系统管理员补录数据；重新备份数据，并写出故障分析报告。

五、应急处置

发生信息网络突发事件后，相关人员应在最短时间内向网络安全和信息化工作领导小组报告，工作组组织人员开展先期处置，及时消除非法信息、恢复系统。

发生重大事故（事件），无法迅速消除或恢复系统，影响较大时实施紧急关闭，并立即向委党委报告。

六、善后处置

应急处置工作结束后，网络安全和信息化工作领导小组组织有关人员和技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题

进行全面调查评估，根据应急处置中暴露出的管理、协调和技术问题，改进和完善预案，实施针对性演练，总结经验教训，整改存在隐患组织，恢复正常工作秩序。

七、应急保障

（一）通信保障

基层卫生健康和信息化股负责收集、建立网络与信息安全突发事件应急处置工作小组内部及其他相关部门的应急联络信息，网络安全和信息化工作领导小组全体人员保证全天 24 小时通讯畅通。

（二）装备保障

基层卫生健康和信息化股负责建立并保持电力、空调、机房等网络安全运行基本环境，预留一定数量的信息网络硬件和软件设备，指定专人保管和维护。

（三）数据保障

重要信息系统均应建立备份系统，保证重要数据在受到破坏后可紧急恢复。

（四）队伍保障

建立符合要求的网络与信息安全保障技术支持力量，对网络接入单位的网络与信息安全保障工作人员提供技术支持和培训服务。

八、监督管理

（一）宣传教育和培训

将网络与信息安全突发事件的应急管理、工作流程等列为培训内容，增强应急处置工作中的组织能力。加强对网络与信息安全突发事件的技术准备培训，提高技术人员的防范意识及技能。网络安全和信息化工作领导小组每年至少开展一次全委范围内的信息网络安全教育，提高信息安全防范意识和能力。

（二）预案演练

网络安全和信息化工作领导小组每年至少安排一次演练，建立应急预案定期演练制度。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

（三）责任与奖惩

按照预案的要求，网络安全和信息化工作领导小组不定期对各项制度、计划、方案、人员及物资等进行检查，对在突发信息网络时间应急处置中做出突出贡献的集体和个人，提出表彰奖励建议；对玩忽职守，造成不良影响或严重后果的，依法依规提出处理意见建议，并追究其责任。

九、附则

（一）预案更新

结合信息网络快速发展和经济社会发展状况，配合相关法律法规的制定、修改和完善，适时修订本预案。

（二）制定和解释

本预案由网络安全和信息化工作领导小组制定并解释。

（三）预案实施

本预案由委党委批准后实施。

桐柏县卫生健康委员会

2021 年 3 月 29 日